ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

A MODIFIED MIMO WIRELESS SECURE COMMUNICATION USING HOMOPHONIC CODE DESIGN

Priya.J[1] (Assistant professor)Baby.M[2],Suganya.D[3],Susithra.M[4],Vanithamani.R[5]

Assistant Professor[1], UG Scholar[2, 3, 4, 5]

Department of ECE

VSB College of Engineering Technical Campus

Kinathukadavu, Coimbatore, Tamil Nadu, India

Abstract – In wireless communication MIMO (Multiple Input Multiple Output) is an antenna technology. The channel estimation can provide a source of randomness which provides secret key generation (SKG) to both sender and receiver. The SKG method is based on both phase difference and time delay in wide band transmission. The data can be secured by using transmission of artificial noise in null space. There exist a Gaussian channel estimation error. Homophonic code is used because of its reliability and security and also it consumes less power. Our proposed method is to enhance data and its secrecy rate by combining the encryption and encoding in addition to that Artificial Noise(AN). The combination of encryption and encoding will improves the secrecy rate of data transmission. The encrypted symbols at the transmitter side act as message for receiver and noise for eavesdroppers. Before transmitting a data, we have to set the threshold value. Based on the threshold value, we can decide whether our data is secure or not. We first analyze the keys can be instantaneously extracted by using channel measurements in order to overcome the problem of low secret key bit allocation. We demonstrate the improvements in secret communication rates using a simple uniform power allocation strategy.

Index Terms – Secret Key Generation (SKG), Channel State Information (CSI), Data Carrying Artificial Noise (DCAN), One Time Pad (OTP), Secrecy, zero-mean circularly-symmetric complex Gaussian (ZMCSCG).

I.INTRODUCTION

The broadcast nature of wireless communication makes privacy and deep-rooted concern. The wireless channel used for secret key generation (SKG) has attracted recent interest. Wireless channels are considered as a reciprocal for a given frequency. The properties of multipath are identical in both transmitter side as well as receiver side direction link.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

At the same frequency , the training signals that can be exchanged in both direction where as the temporal variations of the fading coefficients provides a source of randomness is observed on the two ends of the link from which ,a two identical keys are extracted. The received signal properties have been attempted in many times with the help of key agreement from wireless channel. Signal amplitude is often used because of its ease of computation. Fading channels in rich scattering environments are known also to decorrelate quickly in space; distances more than 1/2 of a wavelength are generally assumed to produce significantly uncorrelated channels. Thus, the wireless channel has an important property of being uniquely observable by Alice and Bob, and is therefore invulnerable to discovery by any

III. DCAN WITH ERROR-FREE CSI

In this section, we make the following assumptions about CSI:

A1. Both Alice and Bob have full, instantaneous, and error free knowledge of the main channel matrix H, and know the statistics of the eavesdropper channel G but have no knowledge of any specific realization.

A2. Eve has full, instantaneous and error-free knowledge of the eavesdropper channel G and of the right singular vector matrix V of the main channel. Note that in much of the existing AN literature, the worst case scenario where Eve has full knowledge of H is commonly assumed. Assumption of known eavesdropper channel statistics is very common in existing literature corresponds to the scenario.

ye = GVs + ne;

Where Eve's environmental surroundings match those of Alice and Bob, and thus yield an eavesdropper channel independent and identical for distributed main channel. However, since Eve is assumed to be passive her exact channel coefficients remain unknown to Alice. Since Eve is able to receive the training signals from Alice, Eve can easily estimate the MIMO channel G between herself and Alice. For a comprehensive treatment of secrecy outage performance given presence of eavesdroppers with locations randomly distributed according to a Poisson point process (PPP), also uses a stochastic geometry approach, and considers probability of achieving secrecy when both the legitimate users (i.e. Alice, Bob) and eavesdroppers randomly distributed according to a PPP. It is clear that, to decode the message symbols, Eve must have not only knowledge of her channel but also partial knowledge of the main channel as well. That is, to arrive at an estimate of s, Eve must not only undo the mixing effects of G but also those effects of V. Eve's best hope of acquiring main-channel state data is to have either Alice or Bob reveal information to her.

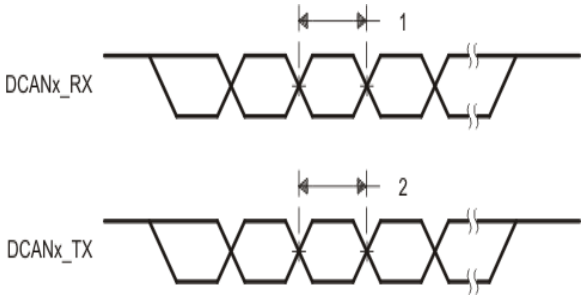

Fig 3 DCAN at Transmitter and Receiver

This might come in the form of feedback during the main channel estimation process. For example, in the LTE standard snooping other party receiving the pilot signals. Secret key agreement from wireless measurements avoids the problem of distributing the keys a priori where it might be ambushed by a mischievous outsider. RSA and other public-key cryptographic methods can be broken by any of the eavesdropper or hacker intercepting transmission given sufficient time and computational power.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

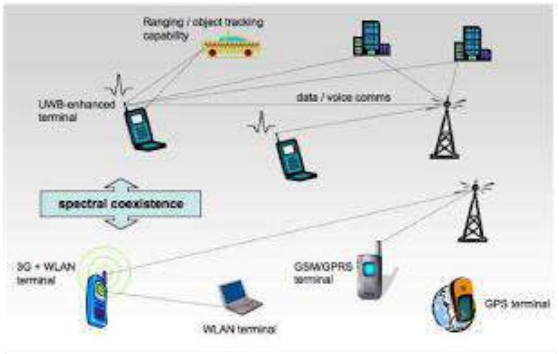

Fig 1 *Secret Key Generation*

Since OTP encryption is by itself generally considered unfeasible for most applications, there have been other efforts at finding new information theoretically secure methods of communication. The secret key generation is simple with efficient power management. There is no use of symmetric key algorithm. Because it requires shared secret key at every end of transmitting and receiving medium. By using homophonic code design secret key bit allocation rate can be improved. Homophonic coding is used to enhance the protection of the key used in the stream. Fully-homophonic encryption schemes may cause learning parity with noise. The LPN problem can be solved by using notion of oracle. The LPN problem asks to recover a secret vector s given access to noisy inner products of itself and random vectors.

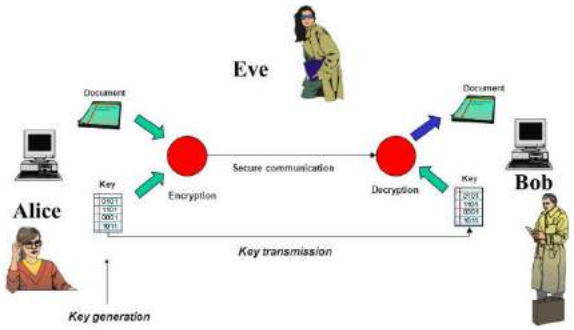

Fig 2 Communication of antennas.

Notation: The following notation is used throughout the paper. Bold-face of lower case type denotes vector a; bold-face of Uppercase type denotes matrix M. jMj, MT, and MH are the matrix determinant, transpose, and Hermitian transpose, respectively. The matrix trace tr(M) denotes the sum of the diagonal elements of M. The identity matrix of size p _ p is denoted Ip. C is the field of complex numbers. The entropy of vector x is h(x); conditional entropy of vector given z is h(xjz). The mutual information between vectors x and y is I(x; y); mutual information conditioned on z is I(x; yjz). The hat symbol ^a denotes the estimate of value a. E_ [_] denotes expectation with respect to the probability distribution on and cov(w) denotes the covariance matrix of a vector w. We use diag(x)to mean a matrix with elements of x along its diagonal and zeros elsewhere; similarly, diag(M1 M2 : : : MK) is a block diagonal matrix constructed from M1;M2; : : : ;MK.

II. SYSTEM MODEL

Define t, r and e as the number of antennas at Alice, Bob, and Eve, respectively. $H \epsilon \mathbb{C}^{r \times t}$ Is the MIMO main (Alice-Bob) channel matrix, and $G \epsilon \mathbb{C}^{e \times t}$ is the MIMO eavesdropper (Alice-Eve) channel matrix. We assume a rich scattering environment such that both channels are flat fading. We further assume the block-fading model, where the coherence time of the channel is large enough that coding can be performed within the transmission interval. The entries of H are independent and identically distributed zero-mean circularly-symmetric complex Gaussian (ZMCSCG). The rich scattering assumption is critical to ensure Eve antenna is not able to gather information during the SKG process and arrive at a well estimate of the secret key. Since experimental results have shown that, in an environment with insufficient reflections, signals received at Eve during the channel estimation phase can be highly connected with the main channel. In this paper we assume Eve's channel coefficients are independent of the main channel coefficients; For fair comparison of different antenna design, we normalize the

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

channel entries $[H]_{i,j} \sim C\mathcal{N}(0,1)$ such that the average received SNR is individualistic, of number of transmit antennas. Alice communicates using a set of constellation points S that approximates a Gaussian input scheme. Alice and Bob begin by estimating the channel and agreeing on a secret key $k \triangleq [k_1, k_2, \dots k_{da}]^T$, with $k_i \in S$. Eve is assumed sufficiently distant from both Alice and Bob such that its probability of guessing the key is no better than chance. Define d_a, d_b and d_c as the respective number of OTP, unencrypted and AN symbols transmitted, and the set $D \triangleq \{d_a, d_b, d_c\}$. Let a $a \triangleq [a_1, a_2, \dots a_{da}]^T$, with $a_i \in S$, be the symbol vector to be encrypted with key k. Define $b \triangleq [b_1, b_2, \dots b_{da}]^T$ and c $\triangleq [c_1, c_2, \dots c_{da}]^T$ as vectors of unencrypted and AN symbols, respectively. Given t antennas, Alice has t degrees of freedom with which to design her transmit vector. At least e degrees of freedom must be devoted to interfering with Eve, and at most r of which can transmit information to Bob. Formally, the requirements on D are,

$$d_b + d_c \leq \text{t} \quad - \quad (1)$$
$$0 < d_a + d_b \leq \text{r} \quad - \quad (2)$$
$$d_a + d_c \geq \text{e} \quad - \quad (3)$$

Bob feeds back to Alice the index of a quantized version of the pre -coding matrix. Given sufficient scattering in the environment and spatial separation (i.e. greater than one-half wavelength distance from both Bob and Alice), it is likely to be overly pessimistic that Eve could reliably know H. In the DCAN scenario considered here, main channel knowledge is gained by reciprocal exchange of training sequences, not by feeding back channel information, and thus Eve is unlikely to have knowledge of V either. One scenario where Eve might have access to knowledge of V is if Alice and Bob are communicating non-sensitive information without encryption using channel feedback and then switch to the DCAN method to protect transmission of sensitive data. To simplify and facilitate analysis, we assume Eve has perfect knowledge of V rather than a quantized version. If Eve knows V, then the expressions we derive are exact; if she does not, then our expressions serve as lower bounds on achievable rates.

III.HOMOPHONIC CODE DESIGN

Maximizing the secrecy of the message sequence for the message has to be encrypted. The security evaluation shows that the computational complexity of recovering the secret key, given all the information a hacker could converge during passive pounce he can mount, is lower bounded by the complexity.

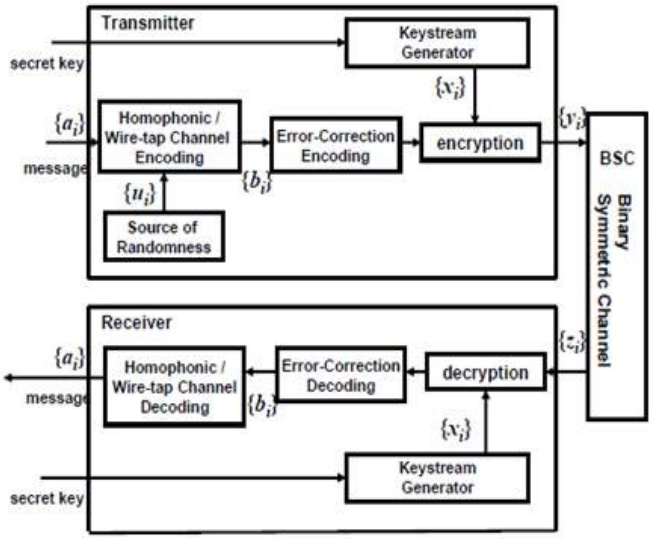

Fig 4 Homophonic wiretap channel

Let k be the private key, let $\mathbf{C_H(\cdot)}$ denote a homophonic encoder, added at the transmitter,

$$\mathbf{u = [u_i]^m_{i=1} \in \{0, 1\}^{m-l}}$$

Let be a vector of pure randomness where each $\mathbf{u_i}$ is the realization of a random variable $\mathbf{U_i}$ with distribution probability **P**. The homophonic encoder is positioned before the error-correcting encoder $\mathbf{C_{ECC}(\cdot)}$, thus out of the **m** bits of data to be sent, **m−l** are replaced by random data, letting actually only **l** bits.

$$\mathbf{a = [a_i]^l_{i=1} \in \{0, 1\}^l}$$

Where a is actual message

$$\mathbf{y = y(k) = C_{ECC}\,(C_H\,(a \| u)) \oplus x}$$

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

as codeword to be sent, where x = x(k) is the output of the key stream generator. Homophonic and error-correction encoding are assumed as linear operations, so that

$$C_H(a||u) = [a||u]G_H$$

Where, G_H is an $m \times m$ matrix, and thus

$$C_{ECC}(C_H(a||u)) = C_{ECC}([a||u]\,G_H = [a||u]\,G_H G_{EC} = [a||u]\,G$$

Where, G_{ECC} is an $m \times n$ binary generator matrix corresponding to $C_{ECC}(\cdot)$, and $G = G_H G_{ECC}$ is an $m \times n$ binary matrix summarizing the two successive encodings at the transmitter.

In this paper we assume that transmission occurs via a binary symmetric channel (BSC) with known
crossover probability p, so that the receiver obtains

$$z = z(k) = y \oplus v = C_{ECC}(C_H(a||u)) \oplus x \oplus v$$

v_i is the realization of a binary random variable V_i with probability **P.** Since receiver knows the private key, the receiver starts with the decryption

$$y = (C_{ECC}(C_H(a||u)) \oplus x \oplus v) \oplus x = C_{ECC}(C_H(a||u)) \oplus v$$

and then decodes

$$C_H(a||u)$$

The decoding is successful, **a** is recovered using C^{-1}_H.

While using the concept of encryption-encoding ,the original data will be secured even though eavesdroppers found the secret key. Threshold value is set before sending information to the receiving medium. Through this technique , we can assure our secrecy rate.

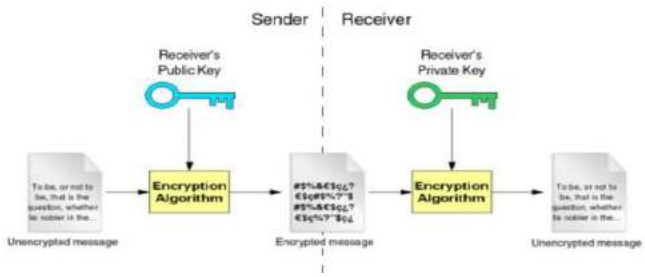

Fig 5 Homophonic code design

IV.PRACTICAL CONSIDERATION

The issues of power allocation, sub channel assignment, secret key bit allocation, secrecy coding and artificial noise. MIMO channels are joining to allocating more power to sub channels with higher SNR, and the less power with low SNR for the total sub channels. The signal to noise ratio is measured at both receiver side as well as the hackers or eavesdroppers side. There is no time delay , because we are sending a noise in the null space. The following figure shows the simulation results in CSI (Channel State Information) and Data Carrying Artificial Noise (DCAN) Error free model.

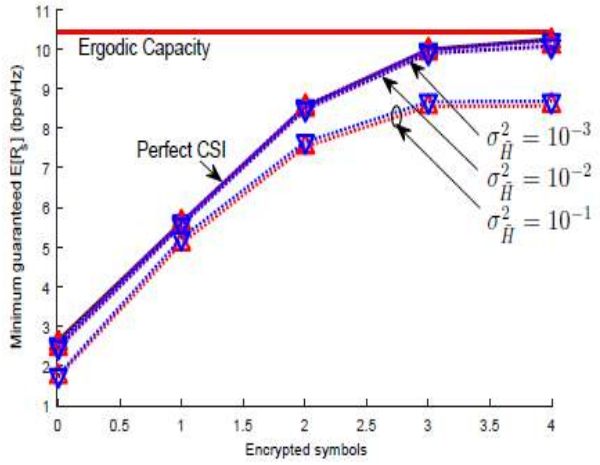

Fig. 6. Bounds on the DCAN minimum achievable secrecy rate with imperfect CSI, for (a) high (20 dB), and (b) low (5 dB) main-channel SNR with t = 8, r = 4, and e = 4. The three sets of bounds shown are for_2~H= f:001; :01; :1g. Red "up" markers (4) indicate the lower bound, and blue "down" markers (5) indicate the upper bound

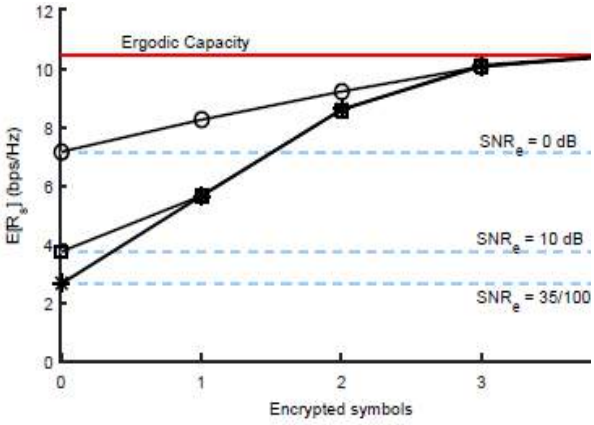

Fig. 7. DCAN achievable rates for a MIMOME system with t = 8, r = 4,and e = 4; uniform power allocation (top) and water filling (bottom) for a main-channel SNR of 5 dB. Dotted lines denote the rates achieved by the AN-only case defined in (21); solid lines with f;_;+; _g markers denote rates achieved with DCAN (20) with respective eavesdropper SNR of
f0; 10; 35; 100g dB.

V.CONCLUSIONS

We have shown how the channel estimation process common to the HCD and KG techniques can be leveraged in a MIMO wiretap channel to enhance achievable secrecy rates and save power over the LPN-only scheme. In AN technique secret key bit allocation is low. We demonstrate the improvements in secret communication rates using a simple uniform power allocation strategy. Our scheme relaxes the common assumption that the eavesdropper has full knowledge of the main channel fading coefficients, and instead assumes only full knowledge of the right singular vector matrix

VI.REFERNCES

[1]. J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," IEEE Trans. On Information Forensics and Security, vol. 5, no. 3, pp. 381 –392, Sep.2010.

[2]. T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi antenna transmission with artificial noise against randomly distributed eavesdroppers," IEEE Transactions on Communications, vol. 63, no. 11, pp. 4347–4362, Nov 2015.

[3]. H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," IEEE Transactions based on Communications, vol. 64, no. 3, pp. 1204–1219, March 2016.

[4]. L. Mirsky, An Introduction to Linear Algebra, Reissue Ed. ed. Dover Publications, Nov. 2011.

[5].Nico D¨ottling, J¨orn M¨uller-Quade, and Anderson C. A. Nascimento. IND-CCA Secure Cryptography Based on a Variant of the LPN Problem. In ASIACRYPT, pages 485–503, 2012.

[6] Alexandre Duc and Serge Vaudenay. HELEN: A Public-Key Cryptosystem Based on the LPN and the Decisional Minimal Distance Problems. In AFRICACRYPT, pages 107–126, 2013.

[7].Marc P. C. Fossorier, Miodrag J. Mihaljevic, Hideki Imai, Yang Cui, and Kanta Matsuura. An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HBProtocols for RFID Authentication. In INDOCRYPT, pages 48–62, 2006.